



PATENT
81754.0041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Michio KOBAYASHI

Serial No. 09/676,347

Confirmation No. 2194

Filed: September 29, 2000

For: Information Authenticating Apparatus
and Authenticating Station

Date of NOA: December 15, 2005

Art Unit: 2132

TRANSMITTAL OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 11-280825 which was filed September 30, 1999, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

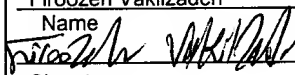
HOGAN & HARTSON L.L.P.

Date: February 22, 2006

By: 

Troy M. Schmelzer
Registration No. 36,667
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450, on
February 22, 2006
Date of Deposit
Firoozeh Vakilzadeh
Name
 2/22/06
Signature Date

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 1 9 9 9 年 9 月 3 0 日

出 願 番 号
Application Number: 平成 1 1 年 特 許 願 第 2 8 0 8 2 5 号

パリ条約による外国への出願
用いる優先権の主張の基礎
となる出願の国コードと出願
番号

country code and number
of your priority application,
which is used for filing abroad
under the Paris Convention, is

J P 1 9 9 9 - 2 8 0 8 2 5

出 願 人
Applicant(s): セイコーエプソン株式会社

BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 6 年 1 月 2 4 日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋





【書類名】 特許願

【整理番号】 J0075969

【提出日】 平成11年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 情報認証装置及び認証局

【請求項の数】 23

【発明者】

 【住所又は居所】 長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

 【氏名】 小林 道夫

【特許出願人】

 【識別番号】 000002369

 【氏名又は名称】 セイコーエプソン株式会社

 【代表者】 安川 英昭

【代理人】

 【識別番号】 100093388

 【弁理士】

 【氏名又は名称】 鈴木 喜三郎

 【連絡先】 0 2 6 6 - 5 2 - 3 1 3 9

【選任した代理人】

 【識別番号】 100095728

 【弁理士】

 【氏名又は名称】 上柳 雅誉

【選任した代理人】

 【識別番号】 100107261

 【弁理士】

 【氏名又は名称】 須澤 修

【手数料の表示】

【予納台帳番号】 013044

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9711684

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報認証装置及び認証局

【特許請求の範囲】

【請求項 1】 データの認証を行う装置であって、

データを入力するデータ入力手段と、外部から取得した情報に基づいて前記データ入力手段でデータを入力したことを認証するための認証情報を生成してこれを前記データ入力手段で入力したデータに付加する認証情報付加手段と、を備えることを特徴とする情報認証装置。

【請求項 2】 請求項 1 において、

前記認証情報付加手段は、外部情報発信手段を利用して位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 3】 デジタル署名を行う認証局を利用してデータの認証を行う装置であって、

データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備えることを特徴とする情報認証装置。

【請求項 4】 請求項 3 において、

前記認証情報付加手段は、時間を測定する時間測定手段を有し、前記時間測定手段で測定した時間に基づいて、前記データ入力手段でデータを入力した時点を特定するための時間情報を生成し、生成した時間情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 5】 請求項 3 及び 4 のいずれかにおいて、

前記認証情報付加手段は、位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 6】 請求項 3 乃至 5 のいずれかにおいて、

前記認証情報付加手段は、周囲の環境状態を測定する環境状態測定手段を有し、前記環境状態測定手段で測定した環境状態に基づいて、前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成し、生成した環境状態情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 7】 請求項 3 乃至 6 のいずれかにおいて、

個人情報記憶するための個人情報記憶手段と、個人情報を入力する個人情報入力手段と、を備え、

前記認証情報付加手段は、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、前記個人情報記憶手段の個人情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 8】 請求項 3 乃至 7 のいずれかにおいて、

当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段を備え、

前記認証情報付加手段は、前記装置情報記憶手段の装置情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 9】 請求項 3 乃至 8 のいずれかにおいて、

前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、当該データに誤りが含まれているか否かを検査するための検査情報を生成し、生成した検査情報を認証情報として付加するようになっていることを特徴とする情報認証装置。

【請求項 10】 請求項 9 において、

前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、ハッシュ関数により検査情報を生成するようになっていることを特徴とする情報認証装置。

【請求項 11】 請求項 3 乃至 10 のいずれかにおいて、

前記認証情報付加手段は、認証情報を付加したデータを暗号化するようになっ

ていることを特徴とする情報認証装置。

【請求項 1 2】 請求項 1 1 において、
前記暗号化方式は、公開鍵暗号化方式であり、
前記認証情報付加手段は、認証情報を付加したデータを当該情報認証装置の秘密鍵で暗号化していることを特徴とする情報認証装置。

【請求項 1 3】 請求項 3 乃至 1 2 のいずれかにおいて、
前記認証局でデジタル署名が付加されたデータを当該認証局から受信する受信手段と、前記受信手段で受信したデータを記憶するデータ記憶手段と、を備えることを特徴とする情報認証装置。

【請求項 1 4】 請求項 3 乃至 1 3 のいずれかに記載の情報認証装置から送信されたデータに対してデジタル署名を行う認証局であって、

前記情報認証装置からデータを受信する認証局側受信手段と、前記認証局側受信手段で受信したデータにデジタル署名を付加するデジタル署名付加手段と、を備え、

前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータに付加された認証情報に基づいて、前記データ入力手段でデータを入力したことを認証したときは、前記認証局側受信手段で受信したデータにデジタル署名を付加していることを特徴とする認証局。

【請求項 1 5】 請求項 1 4 において、
前記デジタル署名付加手段は、時間を測定する認証局側時間測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加していることを特徴とする認証局。

【請求項 1 6】 請求項 1 4 及び 1 5 のいずれかにおいて、
前記デジタル署名付加手段は、前記情報認証装置の位置を測定する認証局側位置測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているときは、前記認証局側受信手段で受信したデ

ータにデジタル署名を付加するようになっていることを特徴とする認証局。

【請求項 1 7】 請求項 1 4 乃至 1 6 のいずれかにおいて、

前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段を備え、

前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっていることを特徴とする認証局。

【請求項 1 8】 請求項 1 4 乃至 1 7 のいずれかにおいて、

前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項 9 記載の情報認証装置と同一の方式により検査情報を生成し、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっていることを特徴とする認証局。

【請求項 1 9】 請求項 1 8 において、

前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項 1 0 記載の情報認証装置と同一のハッシュ関数により検査情報を生成するようになっていることを特徴とする認証局。

【請求項 2 0】 請求項 1 4 乃至 1 9 のいずれかにおいて、

前記デジタル署名付加手段は、請求項 1 1 記載の情報認証装置の暗号化方式と対応する復号化方式により前記認証局側受信手段で受信したデータを復号化するようになっていることを特徴とする認証局。

【請求項 2 1】 請求項 2 0 において、

前記復号化方式は、公開鍵復号化方式であり、

前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを、当該データの送信元である情報認証装置の公開鍵で復号化するようになっていることを特徴とする認証局。

【請求項 2 2】 請求項 1 4 乃至 2 1 のいずれかにおいて、
前記デジタル署名付加手段でデジタル署名を付加したデータを前記情報認証装置に送信する認証局側送信手段を備えることを特徴とする認証局。

【請求項 2 3】 請求項 1 4 乃至 2 1 のいずれかにおいて、
前記デジタル署名付加手段でデジタル署名を付加したデータを記憶する認証局側データ記憶手段を備えることを特徴とする認証局。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データの認証を行う情報認証装置および認証局に係り、特に、データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局に関する。

【0 0 0 2】

【従来の技術】

近年、アメリカ等では、通常のカメラで撮影した写真のほか、デジタルカメラで撮影したデジタル画像も裁判の証拠として認められるようになってきている。しかし、デジタル画像等のデジタルデータは、一般に改ざんが比較的容易であるため、証拠の証明力が不十分であるという問題があった。

【0 0 0 3】

従来、デジタルデータの証拠としての証明力を向上する技術に関連するものとして、例えば、特開平11-115831号公報に開示された車両制御イベントデータ認証装置がある。

【0 0 0 4】

これは、車両事故の発生前、発生中または発生後に運転者によって実行された一連の運転操作等の制御イベントを記録するものであって、制御イベント情報を受信すべく結合され、第1タイム・スタンプおよび車両識別番号VINを制御イベント情報に付加して第1情報を与え、第1情報をタイム・オーバーラップ方式でメモリに出力するマイクロコントローラと、マイクロコントローラおよびマイクロプロセッサに結合され、第1情報および第2情報をタイム・オーバーラップ方式

で格納するメモリと、メモリおよび複数のトランスデューサに結合され、受信した衝突データが以前の衝突データとは異なるかどうかを判定し、受信した衝突データが異なるときは、第2タイム・スタンプおよびVINを受信した衝突データに追加して、第2情報を生成するマイクロプロセッサと、で構成されている。

【0005】

【発明が解決しようとする課題】

しかしながら、上記従来の車両制御イベントデータ認証装置にあっては、内部タイマから取得した値に基づいてタイム・スタンプを生成してこれを制御イベント情報に付加するようになっているため、内部タイマの値が利用者によって変更されたり、経年劣化等の原因により内部タイマの値がずれたりする可能性があり、制御イベント情報の証拠としての証明力が不十分であるという問題があった。

【0006】

また、マイクロコントローラによって記録される制御イベント情報は、マイクロコントローラによって「サイン」が付加される、すなわち、記録された制御イベント情報が特定の車両の運転中に生成されたことを保証するために、タイム・スタンプと所定の識別値とを含むようになっているが、この「サイン」は、内部で独自に生成・付加されるものであるため、客観性に乏しく、これも証拠としての証明力が不十分である。

【0007】

また、パーソナルIDや車両識別番号VINがそのままの状態でもメモリに格納されるため、利用者によって改ざんされる可能性があり、これも証拠としての証明力が不十分である。

【0008】

一方、データの証拠としての証明力を向上する必要性は、裁判だけに限らず、次のような場合にも考えられる。

【0009】

例えば、病院等で検査を行う場合には、いつ誰がどこで検査を行ったかということを証明するデータを記録しておくことが考えられるが、こうしたデータは、患者にとって重要なデータであることから、誰にも改ざんされず、客観性を有し

ていることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要性がある。

【0010】

また例えば、宅配便等で荷物を配送する場合には、いつ誰がどのようなルートをとって配送したかを証明するデータを記録しておくことが考えられるが、こうしたデータは、配送過程で荷物が紛失・破損したときに必要なデータであることから、誰にも改ざんされず、客観性を有していることが望まれる。したがって、この場合は、データの証拠としての証明力を向上する必要性がある。

【0011】

その他の場合としては、事故現場の写真や芸能人のスクープ写真を撮影した場合に撮影者、撮影日または撮影場所を証明するとき、学術調査等で調査データを記録する場合、電話やFAX等で商品またはサービスの注文を受け付けた場合に相手方と注文内容を特定するとき、作曲等をした場合に著作権の発生日を証明するときなどが挙げられる。

【0012】

そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局を提供することを目的としている。

【0013】

【課題を解決するための手段】

上記目的を達成するために、本発明に係る請求項1記載の情報認証装置は、データの認証を行う装置であって、データを入力するデータ入力手段と、外部から取得した情報に基づいて前記データ入力手段でデータを入力したことを認証するための認証情報を生成してこれを前記データ入力手段で入力したデータに付加する認証情報付加手段と、を備える。

【0014】

このような構成であれば、データ入力手段でデータが入力されると、認証情報付加手段により、外部から情報が取得され、取得された情報に基づいて認証情報

が生成され、生成された認証情報がデータ入力手段で入力されたデータに付加される。

【0015】

ここで、データには、画像データ、音声・音楽データ、文書データ、波形データ、その他コンピュータ等の情報処理装置上で利用可能なあらゆるデータが含まれる。以下、請求項3記載の情報認証装置において同じである。

【0016】

また、認証情報付加手段は、外部から取得した情報に基づいて認証情報を生成するようになっていればどのようなものであってもよく、例えば、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、受信した時刻信号に基づいて、データ入力手段でデータを入力した時点特定のための時間情報を認証情報として生成するようになっていてもよいし、複数の周回衛星から時刻信号を受信し、それら時刻信号により示される時刻のずれおよび各周回衛星の周回軌道に基づいて、データ入力手段でデータを入力した地点特定のための位置情報を認証情報として生成するようになっていてもよい。また、前者のように時間情報を生成する場合、電波時計（郵政省で発信しているもの）から時刻信号を受信してもよい。

【0017】

さらに、本発明に係る請求項2記載の情報認証装置は、請求項1記載の情報認証装置において、前記認証情報付加手段は、外部情報発信手段を利用して位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点特定のための位置情報を生成し、生成した位置情報を認証情報として付加するようになっている。

【0018】

このような構成であれば、位置測定手段により、外部情報発信手段を利用して位置が測定され、認証情報付加手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、生成された位置情報が認証情報として付加される。

【0019】

ここで、外部情報発信手段としては、PHS（Personal Handyphone System）

、G S M (Global System for Mobile Communication) 若しくは I M T - 2 0 0 0 に準拠した携帯電話、または G P S (Global Positioning System) が挙げられる。

【 0 0 2 0 】

また、本発明に係る請求項 3 記載の情報認証装置は、デジタル署名を行う認証局を利用してデータの認証を行う装置であって、データを入力するデータ入力手段と、前記データ入力手段でデータを入力したことを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備える。

【 0 0 2 1 】

このような構成であれば、データ入力手段でデータが入力されると、認証情報付加手段により、データ入力手段で入力されたデータに認証情報が付加され、送信手段により、認証情報付加手段で認証情報が付加されたデータが認証局に送信される。そして、認証局により、情報認証装置から送信されたデータに対してデジタル署名が行われる。

【 0 0 2 2 】

ここで、情報認証装置は、認証局にデータを送信した後はどのように動作するようになっていてもよく、例えば、デジタル署名を行ったデータを認証局から受信し、受信したデータを記憶するようになっていてもよいし、デジタル署名を行ったデータを認証局に保持させるようになっていてもよいし、デジタル署名を行ったデータを認証局を経て他の端末に送信するようになっていてもよい。

【 0 0 2 3 】

さらに、本発明に係る請求項 4 記載の情報認証装置は、請求項 3 記載の情報認証装置において、前記認証情報付加手段は、時間を測定する時間測定手段を有し、前記時間測定手段で測定した時間に基づいて、前記データ入力手段でデータを入力した時点を特定するための時間情報を生成し、生成した時間情報を認証情報として付加するようになっている。

【 0 0 2 4 】

このような構成であれば、時間測定手段により、時間が測定され、認証情報付加手段により、時間測定手段で測定された時間に基づいて時間情報が生成され、生成された時間情報が認証情報として付加される。

【 0 0 2 5 】

ここで、時間測定手段は、時間を測定するようになっていればどのようなものであってもよく、例えば、基準時から経過した時間を測定するようになっていてもよいし、現在の時刻を測定するようになっていてもよい。また、周回衛星を利用するなどして、外部から取得した情報により時間を測定するようになっていてもよいし、クロックタイマを内蔵するなどして、内部で生成した情報により時間を測定するようになっていてもよい。

【 0 0 2 6 】

さらに、本発明に係る請求項 5 記載の情報認証装置は、請求項 3 および 4 のいずれかに記載の情報認証装置において、前記認証情報付加手段は、位置を測定する位置測定手段を有し、前記位置測定手段で測定した位置に基づいて、前記データ入力手段でデータを入力した地点を特定するための位置情報を生成し、生成した位置情報を認証情報として付加するようになっている。

【 0 0 2 7 】

このような構成であれば、位置測定手段により、位置が測定され、認証情報付加手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、生成された位置情報が認証情報として付加される。

【 0 0 2 8 】

ここで、位置測定手段は、位置を測定するようになっていればどのようなものであってもよく、例えば、GPS を利用するなどして、外部から取得した情報により位置を測定するようになっていてもよいし、ジャイロおよび加速度計を利用するなどして、内部で生成した情報により位置を測定するようになっていてもよい。

【 0 0 2 9 】

さらに、本発明に係る請求項 6 記載の情報認証装置は、請求項 3 ないし 5 のい

ずれかに記載の情報認証装置において、前記認証情報付加手段は、周囲の環境状態を測定する環境状態測定手段を有し、前記環境状態測定手段で測定した環境状態に基づいて、前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成し、生成した環境状態情報を認証情報として付加するようになっている。

【 0 0 3 0 】

このような構成であれば、環境状態測定手段により、周囲の環境状態が測定され、認証情報付加手段により、環境状態測定手段で測定された環境状態に基づいて環境状態情報が生成され、生成された環境状態情報が認証情報として付加される。

【 0 0 3 1 】

ここで、環境状態測定手段は、周囲の環境状態を測定するようになっていればどのようなものであってもよく、例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量を測定するようになっていけばよい。

【 0 0 3 2 】

さらに、本発明に係る請求項 7 記載の情報認証装置は、請求項 3 ないし 6 のいずれかに記載の情報認証装置において、個人情報記憶するための個人情報記憶手段と、個人情報を入力する個人情報入力手段と、を備え、前記認証情報付加手段は、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、前記個人情報記憶手段の個人情報を認証情報として付加するようになっている。

【 0 0 3 3 】

このような構成であれば、個人情報入力手段で個人情報が入力されると、入力された個人情報と個人情報記憶手段の個人情報とが所定関係を満たしているときは、個人情報記憶手段の個人情報が認証情報として付加される。

【 0 0 3 4 】

ここで、個人情報としては、例えば、個人ごとに割り当てられた I D コード、血液型や指紋等の個人の人体の特徴に依存した情報、または住所や電話番号等の個人の生活環境に依存した情報が挙げられる。

【 0 0 3 5 】

また、所定関係を満たすことには、例えば、照合対象の個人情報と被照合対象の個人情報とが一致していること、照合対象の個人情報を用いて所定演算式により演算を行った結果が被照合対象の個人情報と一致していること、または照合対象の個人情報を用いて所定演算式により演算を行った結果と被照合対象の個人情報を用いて所定演算式により演算を行った結果が一致すること、が挙げられる。

【 0 0 3 6 】

また、個人情報記憶手段は、個人情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ個人情報を記憶しておいてもよいし、本装置の動作時に個人情報を記憶するようにしてもよい。

【 0 0 3 7 】

さらに、本発明に係る請求項 8 記載の情報認証装置は、請求項 3 ないし 7 のいずれかに記載の情報認証装置において、当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段を備え、前記認証情報付加手段は、前記装置情報記憶手段の装置情報を認証情報として付加するようになっている。

【 0 0 3 8 】

このような構成であれば、認証情報付加手段により、装置情報記憶手段の装置情報が認証情報として付加される。

【 0 0 3 9 】

ここで、装置情報記憶手段は、装置情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ装置情報を記憶しておいてもよいし、本装置の動作時に装置情報を記憶するようにしてもよい。

【 0 0 4 0 】

さらに、本発明に係る請求項 9 記載の情報認証装置は、請求項 3 ないし 8 のいずれかに記載の情報認証装置において、前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、当該データに誤りが含まれているか否かを検査するための検査情報を生成し、生成した検査情報を認証情報として付加するようになっている。

【 0 0 4 1 】

このような構成であれば、認証情報付加手段により、データ入力手段で入力されたデータを用いて検査情報が生成され、生成された検査情報が認証情報として付加される。

【 0 0 4 2 】

ここで、検査情報とは、データに誤りが含まれているか否かを検査するための情報をいい、こうした情報としては、例えば、パリティチェックコード、群計数チェックコード等の誤り検出符号や、CRC (cyclic redundancy check)、ハミングコード等の誤り訂正符号や、限度検査、合計検査を行うための検査情報や、データを所定の暗号キーで暗号化した暗号化情報を挙げることができる。以下、請求項 1 8 記載の認証局において同じである。

【 0 0 4 3 】

さらに、本発明に係る請求項 1 0 記載の情報認証装置は、請求項 9 記載の情報認証装置において、前記認証情報付加手段は、前記データ入力手段で入力したデータを用いて、ハッシュ関数により検査情報を生成するようになっている。

【 0 0 4 4 】

このような構成であれば、認証情報付加手段により、データ入力手段で入力されたデータを用いてハッシュ関数により検査情報が生成される。

【 0 0 4 5 】

さらに、本発明に係る請求項 1 1 記載の情報認証装置は、請求項 3 ないし 1 0 のいずれかに記載の情報認証装置において、前記認証情報付加手段は、認証情報を付加したデータを暗号化するようになっている。

【 0 0 4 6 】

このような構成であれば、認証情報付加手段により、認証情報が付加されたデータが暗号化される。そして、送信手段により、暗号化されたデータが認証局に送信される。

【 0 0 4 7 】

ここで、暗号化方式は、どのようなものであってもよく、例えば、共通鍵暗号化方式であってもよいし、公開鍵暗号化方式であってもよい。これらの暗号化方

式としては、例えば、ブロック暗号化方式として、D E S (Data Encryption Standard)、R C 5、F E A L等の攪拌・置換型の暗号化方式、またはR S A、エルガマル暗号、D H法、楕円暗号等のべき乗・剰余型の暗号化方式が挙げられ、ストリーム暗号化方式として、R C 4、バーナム暗号、N L F S R等が挙げられる。

【0 0 4 8】

さらに、本発明に係る請求項 1 2 記載の情報認証装置は、請求項 1 1 記載の情報認証装置において、前記暗号化方式は、公開鍵暗号化方式であり、前記認証情報付加手段は、認証情報を付加したデータを当該情報認証装置の秘密鍵で暗号化するようにになっている。

【0 0 4 9】

このような構成であれば、認証情報付加手段により、認証情報が付加されたデータが、その情報認証装置の秘密鍵で暗号化される。

【0 0 5 0】

さらに、本発明に係る請求項 1 3 記載の情報認証装置は、請求項 3 ないし 1 2 のいずれかに記載の情報認証装置において、前記認証局でデジタル署名が付加されたデータを当該認証局から受信する受信手段と、前記受信手段で受信したデータを記憶するデータ記憶手段と、を備える。

【0 0 5 1】

このような構成であれば、受信手段により、送信手段で送信され、認証局でデジタル署名が付加されたデータがその認証局から受信され、受信されたデータがデータ記憶手段に記憶される。

【0 0 5 2】

一方、上記目的を達成するために、本発明に係る請求項 1 4 記載の認証局は、請求項 3 ないし 1 3 のいずれかに記載の情報認証装置から送信されたデータに対してデジタル署名を行う認証局であって、前記情報認証装置からデータを受信する認証局側受信手段と、前記認証局側受信手段で受信したデータにデジタル署名を付加するデジタル署名付加手段と、を備え、前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータに付加された認証情報に基づいて

、前記データ入力手段でデータを入力したことを認証したときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【0053】

このような構成であれば、認証局側受信手段により情報認証装置からデータが受信されると、デジタル署名付加手段により、認証局側受信手段で受信されたデータに付加された認証情報に基づいて、データ入力手段でデータを入力したことが認証されたときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0054】

さらに、本発明に係る請求項 1 5 記載の認証局は、請求項 1 4 記載の認証局において、前記デジタル署名付加手段は、時間を測定する認証局側時間測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【0055】

このような構成であれば、認証局側時間測定手段により、時間が測定され、デジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された時間情報により特定される時間と認証局側時間測定手段で測定された時間とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0056】

ここで、認証局側時間測定手段は、時間を測定するようになっていればどのようなものであってもよく、例えば、基準時から経過した時間を測定するものであってもよいし、現在の時刻を測定するものであってもよい。また、周回衛星を利用するなどして、外部から取得した情報により時間を測定するようになっていてもよいし、クロックタイマを内蔵するなどして、内部で生成した情報により時間を測定するようになっていてもよい。

【 0 0 5 7 】

また、所定関係を満たすことには、例えば、照合対象の時間と被照合対象の時間とが一致していること、照合対象の時間と被照合対象の時間との時間差が所定範囲内であること、が挙げられる。

【 0 0 5 8 】

さらに、本発明に係る請求項 1 6 記載の認証局は、請求項 1 4 および 1 5 のいずれかに記載の認証局において、前記デジタル署名付加手段は、前記情報認証装置の位置を測定する認証局側位置測定手段を有し、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【 0 0 5 9 】

このような構成であれば、認証局側位置測定手段により、情報認証装置の位置が測定され、デジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された位置情報により特定される位置と認証局側位置測定手段で測定された位置とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【 0 0 6 0 】

ここで、認証局側位置測定手段は、情報認証装置の位置を測定するようになっていればどのようなものであってもよく、例えば、情報認証装置の位置測定手段と通信を行うことにより、情報認証装置の位置を直接的に測定するようにしてもよいし、情報認証装置が携帯電話や P H S 等を利用してデータを送信するような場合は、情報認証装置が通信している基地局を特定することにより、情報認証装置の位置を間接的に測定するようにしてもよい。

【 0 0 6 1 】

また、所定関係を満たすことには、例えば、照合対象の位置と被照合対象の位置とが一致していること、照合対象の位置を中心として所定の領域内に被照合対象の位置が含まれていること、被照合対象の位置を中心として所定の領域内に照

合対象の位置が含まれていること、が挙げられる。

【0 0 6 2】

さらに、本発明に係る請求項 1 7 記載の認証局は、請求項 1 4 ないし 1 6 のいずれかに記載の認証局において、前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段を備え、前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【0 0 6 3】

このような構成であれば、デジタル署名付加手段により、認証局側受信手段で受信されたデータの認証情報として付加された装置情報と認証局側装置情報記憶手段の装置情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0 0 6 4】

ここで、所定関係を満たすことには、例えば、照合対象の装置情報と被照合対象の装置情報とが一致していること、照合対象の装置情報を用いて所定演算式により演算を行った結果が被照合対象の装置情報と一致していること、または照合対象の装置情報を用いて所定演算式により演算を行った結果と被照合対象の装置情報を用いて所定演算式により演算を行った結果が一致すること、が挙げられる。

【0 0 6 5】

また、認証局側装置情報記憶手段は、装置情報をあらゆる手段でかつあらゆる時期に記憶するものであり、あらかじめ装置情報を記憶しておいてもよいし、本装置の動作時に装置情報を記憶するようにしてもよい。

【0 0 6 6】

さらに、本発明に係る請求項 1 8 記載の認証局は、請求項 1 4 ないし 1 7 のいずれかに記載の認証局において、前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項 9 記載の情報認証装置と同一の方式

により検査情報を生成し、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【0067】

このような構成であれば、デジタル署名付加手段により、認証局側受信手段で受信されたデータを用いて、請求項9記載の情報認証装置と同一の方式により検査情報が生成され、生成された検査情報と認証局側受信手段で受信されたデータの認証情報として付加された検査情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0068】

ここで、所定関係を満たすことには、例えば、照合対象の検査情報と被照合対象の検査情報とが一致していること、照合対象の検査情報を用いて所定演算式により演算を行った結果が被照合対象の検査情報と一致していること、または照合対象の検査情報を用いて所定演算式により演算を行った結果と被照合対象の検査情報を用いて所定演算式により演算を行った結果が一致すること、が挙げられる。

【0069】

さらに、本発明に係る請求項19記載の認証局は、請求項18記載の認証局において、前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを用いて、請求項10記載の情報認証装置と同一のハッシュ関数により検査情報を生成するようになっている。

【0070】

このような構成であれば、デジタル署名付加手段により、認証局側受信手段で受信されたデータを用いて、請求項10記載の情報認証装置と同一のハッシュ関数により検査情報が生成される。

【0071】

さらに、本発明に係る請求項20記載の認証局は、請求項14ないし19のいずれかに記載の認証局において、前記デジタル署名付加手段は、請求項11記

載の情報認証装置の暗号化方式と対応する復号化方式により前記認証局側受信手段で受信したデータを復号化している。

【0072】

このような構成であれば、デジタル署名付加手段により、請求項 1 1 記載の情報認証装置の暗号化方式と対応する復号化方式により認証局側受信手段で受信されたデータが復号化される。

【0073】

ここで、復号化方式は、どのようなものであってもよく、例えば、共通鍵復号化方式であってもよいし、公開鍵復号化方式であってもよい。これらの復号化方式としては、例えば、上記請求項 1 1 の項目で例示した暗号化方式に対応したものが挙げられる。

【0074】

さらに、本発明に係る請求項 2 1 記載の認証局は、請求項 2 0 記載の認証局において、前記復号化方式は、公開鍵復号化方式であり、前記デジタル署名付加手段は、前記認証局側受信手段で受信したデータを、当該データの送信元である情報認証装置の公開鍵で復号化している。

【0075】

このような構成であれば、デジタル署名付加手段により、認証局側受信手段で受信されたデータが、そのデータの送信元である情報認証装置の公開鍵で復号化される。

【0076】

さらに、本発明に係る請求項 2 2 記載の認証局は、請求項 1 4 ないし 2 1 のいずれかに記載の認証局において、前記デジタル署名付加手段でデジタル署名を付加したデータを前記情報認証装置に送信する認証局側送信手段を備える。

【0077】

このような構成であれば、認証局側送信手段により、デジタル署名付加手段でデジタル署名が付加されたデータが情報認証装置に送信される。

【0078】

さらに、本発明に係る請求項 2 3 記載の認証局は、請求項 1 4 ないし 2 1 のい

ずれかに記載の認証局において、前記デジタル署名付加手段でデジタル署名を付加したデータを記憶する認証局側データ記憶手段を備える。

【0079】

このような構成であれば、デジタル署名付加手段でデジタル署名が付加されたデータが認証局側データ記憶手段に記憶される。

【0080】

以上では、上記目的を達成するための情報認証装置および認証局を提案したが、これに限らず、上記目的を達成するため、次の情報認証システムを提案することもできる。

【0081】

この情報認証システムは、デジタル署名を行う認証局と情報認証装置とをネットワークを介して通信可能に接続したシステムであって、前記情報認証装置は、データを入力するデータ入力手段と、個人情報を入力する個人情報入力手段と、個人情報を記憶するための個人情報記憶手段と、当該情報認証装置に固有の情報である装置情報を記憶するための装置情報記憶手段と、前記データ入力手段でデータを入力したことを認証するための認証情報を前記データ入力手段で入力したデータに付加する認証情報付加手段と、前記認証情報付加手段で認証情報を付加したデータを前記認証局に送信する送信手段と、を備え、前記認証情報付加手段は、時間を測定する時間測定手段と、位置を測定する位置測定手段と、周囲の環境状態を測定する環境状態測定手段と、前記時間測定手段で測定した時間に基づいて前記データ入力手段でデータを入力した時点特定するための時間情報を生成する時間情報生成手段と、前記位置測定手段で測定した位置に基づいて前記データ入力手段でデータを入力した地点特定するための位置情報を生成する位置情報生成手段と、前記環境状態測定手段で測定した環境状態に基づいて前記データ入力手段でデータを入力した時点における環境状態を特定するための環境状態情報を生成する環境状態情報生成手段と、前記データ入力手段で入力したデータを用いて当該データに誤りが含まれているか否かを検査するための検査情報を生成する検査情報生成手段と、を有し、前記個人情報入力手段で入力した個人情報と前記個人情報記憶手段の個人情報とが所定関係を満たしているときは、生成

した時間情報、位置情報、環境状態情報および検査情報を、並びに前記装置情報記憶手段の装置情報および前記個人情報記憶手段の個人情報を認証情報として付加するようになっており、前記認証局は、前記情報認証装置からデータを受信する認証局側受信手段と、前記情報認証装置に固有の情報である装置情報を記憶するための認証局側装置情報記憶手段と、前記認証局側受信手段で受信したデータにデジタル署名を付加するデジタル署名付加手段と、を備え、前記デジタル署名付加手段は、時間を測定する認証局側時間測定手段と、前記情報認証装置の位置を測定する認証局側位置測定手段と、前記認証局側受信手段で受信したデータを用いて前記検査情報生成手段と同一の方式により検査情報を生成する認証局側検査情報生成手段と、を有し、前記認証局側受信手段で受信したデータの認証情報として付加された時間情報により特定される時間と前記認証局側時間測定手段で測定した時間とが所定関係を満たしているとき、前記認証局側受信手段で受信したデータの認証情報として付加された位置情報により特定される位置と前記認証局側位置測定手段で測定した位置とが所定関係を満たしているとき、前記認証局側受信手段で受信したデータの認証情報として付加された装置情報と前記認証局側装置情報記憶手段の装置情報とが所定関係を満たしているとき、および、生成した検査情報と前記認証局側受信手段で受信したデータの認証情報として付加された検査情報とが所定関係を満たしているときは、前記認証局側受信手段で受信したデータにデジタル署名を付加するようになっている。

【 0 0 8 2 】

このような構成であれば、情報認証装置では、データ入力手段でデータが入力されるとともに、個人情報入力手段で個人情報が入力されると、認証情報付加手段により、データ入力手段で入力されたデータに認証情報が付加され、送信手段により、認証情報付加手段で認証情報が付加されたデータが認証局に送信される。

【 0 0 8 3 】

認証情報が付加される過程では、時間情報生成手段により、時間測定手段で測定された時間に基づいて時間情報が生成され、位置情報生成手段により、位置測定手段で測定された位置に基づいて位置情報が生成され、環境情報生成手段によ

り、環境状態測定手段で測定された環境状態に基づいて環境状態情報が生成され、検査情報生成手段により、データ入力手段で入力されたデータを用いて検査情報が生成される。そして、入力された個人情報と個人情報記憶手段の個人情報とが所定関係を満たしているときは、生成された時間情報、位置情報、環境状態情報および検査情報が、並びに装置情報記憶手段の装置情報および個人情報記憶手段の個人情報が認証情報として付加される。

【0084】

一方、認証局では、認証局側受信手段により情報認証装置からデータが受信されると、デジタル署名付加手段により、認証局側受信手段で受信されたデータに付加された認証情報に基づいて、データ入力手段でデータを入力したことが認証されたときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0085】

デジタル署名が付加される過程では、認証局側検査情報生成手段により、認証局側受信手段で受信されたデータを用いて検査情報生成手段と同一の方式により検査情報が生成される。そして、認証局側受信手段で受信されたデータの認証情報として付加された時間情報により特定される時間と認証局側時間測定手段で測定された時間とが所定関係を満たしているとき、認証局側受信手段で受信されたデータの認証情報として付加された位置情報により特定される位置と認証局側位置測定手段で測定された位置とが所定関係を満たしているとき、認証局側受信手段で受信されたデータの認証情報として付加された装置情報と認証局側装置情報記憶手段の装置情報とが所定関係を満たしているとき、および、生成された検査情報と認証局側受信手段で受信されたデータの認証情報として付加された検査情報とが所定関係を満たしているときは、認証局側受信手段で受信されたデータにデジタル署名が付加される。

【0086】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら説明する。図1ないし図5は、本発明に係る情報認証装置および認証局の形態を示す図である。

【0087】

この実施の形態は、本発明に係る情報認証装置および認証局を、図1に示すように、デジタルカメラ10で取り込んだデジタル画像であるデジタルデータの認証を行う場合について適用したものである。

【0088】

まず、本発明に係る情報認証装置および認証局を適用する情報認証システムの構成を図1を参照しながら説明する。図1は、情報認証システムの構成を示すブロック図である。

【0089】

この情報認証システムは、図1に示すように、デジタル署名を行う認証局200と情報認証装置100とをネットワークを介して通信可能に接続して構成されている。情報認証装置100は、例えば、通常時は認証局200と接続しておらず、デジタルデータの認証を行うときにのみ認証局200と接続するようになっている。なお、発明の理解を容易にするため、情報認証装置100を1台しか図示していないが、実際には、異なる複数の情報認証装置が認証局200に接続可能となっている。

【0090】

情報認証装置100は、デジタル画像であるデジタルデータを取り込むデジタルカメラ10と、個人情報を入力する個人情報入力装置12と、個人情報を記憶した個人情報記憶装置14と、情報認証装置100に固有の情報である装置情報を記憶した装置情報記憶装置16と、デジタルカメラ10でデジタルデータを取り込んだことを認証するための認証情報をデジタルカメラ10で取り込んだデジタルデータに付加する認証情報付加部120と、認証局200とネットワークを介して通信する通信装置18と、認証局200でデジタル署名が付加されたデジタルデータを記憶するデータ記憶装置20と、データ記憶装置20のデジタルデータを外部に出力するための出力端子22と、で構成されている。

【0091】

個人情報入力装置12は、キーボード等の入力デバイスからなり、情報認証装

置 1 0 0 を利用する各利用者ごとに割り当てられた I D と、その I D に対応したパスワードと、を入力するようになっている。

【 0 0 9 2 】

個人情報記憶装置 1 4 には、情報認証装置 1 0 0 を利用する各利用者ごとに割り当てられた I D と、その I D に対応したパスワードと、を暗号化した暗号化個人情報が格納されている。ここで、I D およびパスワードは、例えば、認証局 2 0 0 において、個人 I D 用の暗号化アルゴリズムにより暗号化されたものである。

【 0 0 9 3 】

装置情報記憶装置 1 6 には、情報認証装置 1 0 0 に固有の情報である装置情報（例えば、装置固有の番号）を暗号化した暗号化装置情報が格納されている。ここで、装置情報は、例えば、認証局 2 0 0 において、装置用の暗号化アルゴリズムにより暗号化されたものである。

【 0 0 9 4 】

通信装置 1 8 は、携帯電話や P H S 等を利用して、現在地点から最も近くにある基地局を特定し、無線により一般公衆回線網を通じてネットワークに接続し、そのネットワークを介してデジタルデータを認証局 2 0 0 に送信するようになっている。

【 0 0 9 5 】

次に、認証情報付加部 1 2 0 の構成を詳細に説明する。

【 0 0 9 6 】

認証情報付加部 1 2 0 は、時間を測定する時間測定装置 4 2 と、位置を測定する位置測定装置 4 4 と、周囲の環境状態を測定する複数のセンサ $S_1 \sim S_n$ と、個人情報入力装置 1 2 で入力した個人情報と個人情報記憶装置 1 4 の個人情報とを照合して利用者の認証を行う利用者認証装置 4 6 と、認証情報を生成してこれをデジタルカメラ 1 0 で取り込んだデジタルデータに付加する処理を行う情報処理装置 4 0 と、で構成されている。

【 0 0 9 7 】

時間測定装置 4 2 は、現在の時刻を示す時刻信号を送信する周回衛星から時刻

信号を受信し、受信した時刻信号に基づいて、現在の時刻を測定するようになっている。

【0098】

位置測定装置 44 は、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、それら時刻信号により示される時刻のずれおよび各周回衛星の周回軌道に基づいて、位置を測定するいわゆる GPS を利用して、現在地点の位置を測定するようになっている。

【0099】

センサ $S_1 \sim S_n$ は、周囲の環境状態として、例えば、周囲の温度、湿度、気圧、ガス濃度、風速、標高、音量または光量を測定するようになっている。これらの物理量を測定するセンサとしては、既知の計測器を用いることができる。

【0100】

利用者認証装置 46 は、情報処理装置 40 から利用者の認証要求があったときは、個人情報入力装置 12 で ID およびパスワードを入力するとともに、個人情報記憶装置 14 から暗号化個人情報を読み出してこれを復号化し、入力した ID およびパスワードと、復号化した ID およびパスワードと、が一致するか否かを判定するようになっている。判定の結果、これらが一致すると判定されたときは、正当な利用者であることを示す利用者認証データを情報処理装置 40 に出力し、これらが一致しないと判定されたときは、不正な利用者であることを示す利用者認証データを情報処理装置 40 に出力するようになっている。

【0101】

次に、情報処理装置 40 の構成を図 2 を参照しながら説明する。図 2 は、情報処理装置 40 の構成を示すブロック図である。

【0102】

情報処理装置 40 は、図 2 に示すように、制御プログラムに基づいて演算およびシステム全体を制御する CPU 60 と、所定領域にあらかじめ CPU 60 の制御プログラム等を格納している ROM 62 と、ROM 62 等から読み出したデータや CPU 60 の演算過程で必要な演算結果を格納するための RAM 64 と、外部装置に対してデータの入出力を媒介する I/F 68 と、で構成されており、こ

れらは、データを転送するための信号線であるバス 6 9 で相互にかつデータ授受可能に接続されている。

【0 1 0 3】

I / F 6 8 には、外部装置として、デジタルカメラ 1 0 と、個人情報記憶装置 1 4 と、装置情報記憶装置 1 6 と、通信装置 1 8 と、データ記憶装置 2 0 と、出力端子 2 2 と、時間測定装置 4 2 と、位置測定装置 4 4 と、センサ $S_1 \sim S_n$ と、利用者認証装置 4 6 と、が接続されている。

【0 1 0 4】

C P U 6 0 は、マイクロプロセッシングユニット M P U 等からなり、電源が投入されたときは、R O M 6 2 の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、図 3 のフローチャートに示す認証情報付加処理を実行するようになっている。図 3 は、認証情報付加処理を示すフローチャートである。

【0 1 0 5】

認証情報付加処理は、I / F 6 8 に接続された外部装置を利用して認証情報を生成し、生成した認証情報をデジタルカメラ 1 0 で取り込んだデジタルデータに付加する処理であって、C P U 6 0 において実行されると、図 3 に示すように、まず、ステップ S 1 0 0 に移行するようになっている。

【0 1 0 6】

ステップ S 1 0 0 では、利用者の認証要求を利用者認証装置 4 6 に出力し、ステップ S 1 0 2 に移行して、利用者認証データを利用者認証装置 4 6 から入力し、入力した利用者認証データが正当な利用者であることを示しているか否かを判定し、正当な利用者であることを示していると判定されたとき (Yes) は、ステップ S 1 0 4 に移行する。

【0 1 0 7】

ステップ S 1 0 4 では、デジタル画像であるデジタルデータをデジタルカメラ 1 0 から入力したか否かを判定し、デジタルデータを入力したと判定したとき (Yes) は、ステップ S 1 0 6 に移行して、時間測定装置 4 2 から現在の時刻を入力し、入力した時刻に基づいて、デジタルカメラ 1 0 でデジタルデー

タを入力した時点をも特定するための時間情報を生成し、ステップ S 1 0 8 に移行する。

【0 1 0 8】

ステップ S 1 0 8 では、位置測定装置 4 4 から現在地点の位置を入力し、入力した位置に基づいて、デジタルカメラ 1 0 でデジタルデータを入力した地点を特定するための位置情報を生成し、ステップ S 1 1 0 に移行して、センサ $S_1 \sim S_n$ から周囲の環境状態を入力し、入力した環境状態に基づいて、デジタルカメラ 1 0 でデジタルデータを入力した時点における環境状態を特定するための環境状態情報を生成し、ステップ S 1 1 2 に移行する。

【0 1 0 9】

ステップ S 1 1 2 では、個人情報記憶装置 1 4 から個人情報を読み出し、ステップ S 1 1 4 に移行して、装置情報記憶装置 1 6 から装置情報を読み出し、ステップ S 1 1 6 に移行して、生成した時間情報、位置情報および環境状態情報を、並びに読み出した個人情報および装置情報を認証情報としてデジタルカメラ 1 0 で入力したデジタルデータに付加し、ステップ S 1 1 8 に移行する。具体的にステップ S 1 1 6 では、例えば、認証情報を電子透かしやサブリミナル情報としてデジタルデータに付加する。

【0 1 1 0】

ステップ S 1 1 8 では、認証情報を付加したデジタルデータを所定のハッシュ関数に代入することにより、そのデジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、ステップ S 1 2 0 に移行して、生成した検査情報を認証情報としてデジタルカメラ 1 0 で入力したデジタルデータにさらに付加し、ステップ S 1 2 2 に移行する。具体的にステップ S 1 2 2 では、例えば、認証情報を電子透かしやサブリミナル情報としてデジタルデータに付加する。

【0 1 1 1】

ステップ S 1 2 2 では、公開鍵暗号化方式により、認証情報を付加したデジタルデータを情報認証装置 1 0 0 の秘密鍵で暗号化し、ステップ S 1 2 4 に移行して、暗号化したデジタルデータを通信装置 1 8 に出力して認証局 2 0 0 に送

信し、ステップ S 1 2 6 に移行する。

【0 1 1 2】

ステップ S 1 2 6 では、認証局 2 0 0 でデジタル署名が付加されたデジタルデータを認証局 2 0 0 から受信して通信装置 1 8 から入力したか否かを判定し、デジタル署名が付加されたデジタルデータを入力したと判定されたとき (Yes) は、ステップ S 1 2 8 に移行して、入力したデジタルデータをデータ記憶装置 2 0 に格納し、ステップ S 1 3 0 に移行する。

【0 1 1 3】

ステップ S 1 3 0 では、デジタルデータの出力要求が利用者からあるか否かを判定し、デジタルデータの出力要求があると判定されたとき (Yes) は、ステップ S 1 3 2 に移行して、データ記憶装置 2 0 のデジタルデータを出力端子 2 2 に出力し、ステップ S 1 0 4 に移行する。

【0 1 1 4】

一方、ステップ S 1 3 0 で、デジタルデータの出力要求が利用者からないと判定されたとき (No) は、ステップ S 1 0 4 に移行する。

【0 1 1 5】

一方、ステップ S 1 2 6 で、デジタル署名が付加されたデジタルデータを通信装置 1 8 から入力しないと判定されたとき (No) は、デジタルデータを入力するまでステップ S 1 2 6 で待機する。

【0 1 1 6】

一方、ステップ S 1 0 4 で、デジタルカメラ 1 0 からデジタルデータを入力しないと判定されたとき (No) は、ステップ S 1 3 0 に移行する。

【0 1 1 7】

一方、ステップ S 1 0 2 で、利用者認証データが不正な利用者であることを示していると判定されたとき (No) は、ステップ S 1 3 4 に移行して、強制的に電源を遮断し、一連の処理を終了する。

【0 1 1 8】

次に、図 1 に戻り、認証局 2 0 0 の構成を説明する。

【 0 1 1 9 】

認証局 2 0 0 は、図 1 に示すように、情報認証装置 1 0 0 とネットワークを介して通信する通信装置 2 4 と、個人情報記憶装置 2 6 と、装置情報を記憶した装置情報記憶装置 2 8 と、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するデジタル署名付加部 2 2 0 と、で構成されている。

【 0 1 2 0 】

個人情報記憶装置 2 6 には、個人情報記憶装置 1 4 に格納されているものと同じの I D およびパスワードであって、装置情報記憶装置 2 8 の装置情報により特定される情報認証装置を利用する各利用者ごとに割り当てられた I D と、その I D に対応したパスワードと、が格納されている。また、個人情報記憶装置 2 6 の個人情報は、装置情報記憶装置 2 8 の装置情報と関連づけられており、すなわち、その関連づけにより、装置情報記憶装置 2 8 の装置情報により特定される情報認証装置について、その利用者の I D およびパスワードを特定することが可能となる。なお、この関連づけは、情報認証装置 1 0 0 を利用しようとする者が、利用する前に認証局 2 0 0 に届け出ることにより行われる。

【 0 1 2 1 】

次に、デジタル署名付加部 2 2 0 の構成を詳細に説明する。

【 0 1 2 2 】

デジタル署名付加部 2 2 0 は、時間を測定する時間測定装置 5 2 と、情報認証装置 1 0 0 の位置を測定する位置測定装置 5 4 と、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加する処理を行う情報処理装置 5 0 と、で構成されている。

【 0 1 2 3 】

時間測定装置 5 2 は、時間測定装置 4 2 と同一機能を有して構成されており、現在の時刻を示す時刻信号を送信する周回衛星から時刻信号を受信し、受信した時刻信号に基づいて、現在の時刻を測定するようになっている。

【 0 1 2 4 】

位置測定装置 5 4 は、通信装置 2 4 が情報認証装置 1 0 0 と通信を行っている

間に、情報認証装置 1 0 0 が通信している基地局を特定することにより、情報認証装置 1 0 0 の位置を測定するようになっている。なお、基地局の特定方法は、従来の方法による。

【 0 1 2 5 】

次に、情報処理装置 5 0 の構成を図 4 を参照しながら説明する。図 4 は、情報処理装置 5 0 の構成を示すブロック図である。

【 0 1 2 6 】

情報処理装置 5 0 は、図 4 に示すように、制御プログラムに基づいて演算およびシステム全体を制御する CPU 7 0 と、所定領域にあらかじめ CPU 7 0 の制御プログラム等を格納している ROM 7 2 と、ROM 7 2 等から読み出したデータや CPU 7 0 の演算過程で必要な演算結果を格納するための RAM 7 4 と、外部装置に対してデータの入出力を媒介する I / F 7 8 と、で構成されており、これらは、データを転送するための信号線であるバス 7 9 で相互にかつデータ授受可能に接続されている。

【 0 1 2 7 】

I / F 7 8 には、外部装置として、通信装置 2 4 と、個人情報記憶装置 2 6 と、装置情報記憶装置 2 8 と、時間測定装置 5 2 と、位置測定装置 5 4 と、が接続されている。

【 0 1 2 8 】

CPU 7 0 は、マイクロプロセッシングユニット MPU 等からなり、ROM 7 2 の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、常時、図 5 のフローチャートに示すデジタル署名付加処理を実行するようになっている。図 5 は、デジタル署名付加処理を示すフローチャートである。

【 0 1 2 9 】

デジタル署名付加処理は、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加する処理であって、CPU 7 0 において実行されると、図 5 に示すように、まず、ステップ S 2 0 0 に移行するようになっている。

【0 1 3 0】

ステップ S 2 0 0 では、デジタルデータを情報認証装置 1 0 0 から受信して通信装置 2 4 から入力したか否かを判定し、デジタルデータを入力したと判定されたとき (Yes) は、ステップ S 2 0 2 に移行して、公開鍵復号化方式により、入力したデジタルデータを、そのデジタルデータの送信元である情報認証装置 1 0 0 の公開鍵で復号化し、ステップ S 2 0 4 に移行する。

【0 1 3 1】

ステップ S 2 0 4 では、時間測定装置 5 2 から現在の時刻を入力し、復号化したデジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置 5 2 から入力した時刻との時間差が所定範囲内（例えば、1 分）であるか否かを判定し、その時間差が所定範囲内であると判定されたとき (Yes) は、ステップ S 2 0 6 に移行する。

【0 1 3 2】

ステップ S 2 0 6 では、デジタルデータの送信元である情報認証装置 1 0 0 の位置を位置測定装置 5 4 から入力し、復号化したデジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置 5 4 から入力した位置を中心として所定範囲（例えば、半径 3 0 0 m）の領域内に含まれているか否かを判定し、所定範囲の領域内に含まれていると判定されたとき (Yes) は、ステップ S 2 0 8 に移行する。

【0 1 3 3】

ステップ S 2 0 8 では、復号化したデジタルデータの認証情報として付加された装置情報を復号化し、ステップ S 2 1 0 に移行して、復号化した装置情報をもとに装置情報記憶装置 2 8 を検索し、ステップ S 2 1 2 に移行して、復号化した装置情報に該当する装置情報を索出したか否かを判定し、該当する装置情報を索出したと判定されたとき (Yes) は、ステップ S 2 1 4 に移行する。

【0 1 3 4】

ステップ S 2 1 4 では、復号化したデジタルデータの認証情報として付加された個人情報を復号化し、ステップ S 2 1 6 に移行して、ステップ S 2 1 2 で索出した装置情報をもとに、個人情報記憶装置 2 6 を検索して関連する個人情報を

読み出し、ステップ S 2 1 8 に移行して、復号化した個人情報である I D およびパスワードと、読み出した個人情報である I D およびパスワードと、が一致しているか否かを判定し、これらが一致していると判定されたとき (Yes) は、ステップ S 2 2 0 に移行する。

【 0 1 3 5 】

ステップ S 2 2 0 では、復号化したデジタルデータのうち認証情報として付加された検査情報を除いた部分を、上記ステップ S 1 1 8 と同一のハッシュ関数に代入することにより、そのデジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、ステップ S 2 2 2 に移行して、生成した検査情報と、復号化したデジタルデータの認証情報として付加された検査情報と、が一致しているか否かを判定し、これらが一致していると判定されたとき (Yes) は、ステップ S 2 2 4 に移行する。

【 0 1 3 6 】

ステップ S 2 2 4 では、復号化したデジタルデータにデジタル署名を付加し、ステップ S 2 2 6 に移行して、公開鍵暗号化方式により、デジタル署名を付加したデジタルデータを認証局 2 0 0 の秘密鍵で暗号化し、ステップ S 2 2 8 に移行して、暗号化したデジタルデータを通信装置 2 4 に出力して、そのデジタルデータの送信元である情報認証装置 1 0 0 に送信し、ステップ S 2 0 0 に移行する。

【 0 1 3 7 】

一方、ステップ S 2 2 2 では、ハッシュ関数により生成した検査情報と、復号化したデジタルデータの認証情報として付加された検査情報と、が一致していないと判定されたとき (No) は、不正なデジタルデータであるとしてデジタル署名を付加せず、ステップ S 2 0 0 に移行する。

【 0 1 3 8 】

一方、ステップ S 2 1 8 では、復号化した個人情報である I D およびパスワードと、読み出した個人情報である I D およびパスワードと、が一致していないと判定されたとき (No) は、不正なデジタルデータであるとしてデジタル署名を

付加せず、ステップ S 2 0 0 に移行する。

【0 1 3 9】

一方、ステップ S 2 1 2 では、復号化した装置情報に該当する装置情報を装置情報記憶装置 2 8 から索出しないと判定されたとき (No) は、不正なデジタルデータであるとしてデジタル署名を付加せず、ステップ S 2 0 0 に移行する。

【0 1 4 0】

一方、ステップ S 2 0 6 では、復号化したデジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置 5 4 から入力した位置を中心として所定範囲の領域内に含まれていないと判定されたとき (No) は、不正なデジタルデータであるとしてデジタル署名を付加せず、ステップ S 2 0 0 に移行する。

【0 1 4 1】

一方、ステップ S 2 0 4 では、復号化したデジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置 5 2 から入力した時刻との時間差が所定範囲外であると判定されたとき (No) は、不正なデジタルデータであるとしてデジタル署名を付加せず、ステップ S 2 0 0 に移行する。

【0 1 4 2】

一方、ステップ S 2 0 0 では、デジタルデータを通信装置 2 4 から入力しないと判定されたとき (No) は、デジタルデータを入力するまでステップ S 2 0 0 で待機する。

【0 1 4 3】

次に、上記実施の形態の動作を説明する。

【0 1 4 4】

利用者は、デジタルカメラ 1 0 でデジタル画像を取り込むには、まず、情報認証装置 1 0 0 に電源を投入し、I D およびパスワードを個人情報入力装置 1 2 から入力する。

【0 1 4 5】

ここで、利用者が認証局 2 0 0 に届け出た正当な I D およびパスワードを入力したものとすると、情報認証装置 1 0 0 では、利用者認証装置 4 6 により、個人

情報記憶装置 1 4 から暗号化個人情報を読み出されてこれが復号化され、個人情報入力装置 1 2 から入力された I D およびパスワードと、復号化された I D およびパスワードと、が一致するので、正当な利用者であることを示す利用者認証データが情報処理装置 4 0 に出力される。情報処理装置 4 0 では、正当な利用者であることを示す利用者認証データが入力されると、C P U 6 0 により、ステップ S 1 0 0, S 1 0 2 を経て、正当な利用者であると認証され、デジタルカメラ 1 0 でデジタル画像を取り込み可能な状態となる。

【0 1 4 6】

この状態で、利用者がデジタルカメラ 1 0 でデジタル画像を取り込むと、情報処理装置 4 0 では、デジタルカメラ 1 0 からデジタルデータが入力されるので、ステップ S 1 0 6 ~ S 1 1 6 を経て、時間測定装置 4 2 で測定された時刻に基づいて時間情報が生成され、位置測定装置 4 4 で測定された位置に基づいて位置情報が生成され、センサ $S_1 \sim S_n$ で測定された環境状態に基づいて環境状態情報が生成される。次いで、個人情報記憶装置 1 4 から個人情報を読み出され、装置情報記憶装置 1 6 から装置情報が読み出され、生成された時間情報、位置情報および環境状態情報が、並びに読み出された個人情報および装置情報が認証情報としてデジタルカメラ 1 0 で入力されたデジタルデータに付加される。

【0 1 4 7】

次いで、ステップ S 1 1 8 ~ S 1 2 4 を経て、認証情報が付加されたデジタルデータを用いてハッシュ関数により検査情報がハッシュ値として生成され、生成された検査情報が認証情報としてデジタルカメラ 1 0 で入力されたデジタルデータにさらに付加され、認証情報が付加されたデジタルデータが情報認証装置 1 0 0 の秘密鍵で暗号化され、暗号化されたデジタルデータが通信装置 1 8 に出力される。そして、通信装置 1 8 により、現在地点から最も近くにある基地局が特定され、無線により一般公衆回線網を通じてネットワークに接続され、そのネットワークを介してデジタルデータが認証局 2 0 0 に送信される。

【0 1 4 8】

一方、認証局 2 0 0 では、通信装置 2 4 により、情報認証装置 1 0 0 からデジタルデータが受信されると、受信されたデジタルデータが情報処理装置 5 0

に出力される。情報処理装置 5 0 では、デジタルデータが通信装置 2 4 から入力されると、CPU 7 0 により、ステップ S 2 0 2, S 2 0 4 を経て、入力されたデジタルデータが情報認証装置 1 0 0 の公開鍵で復号化され、復号化されたデジタルデータの認証情報として付加された時間情報により特定される時刻と時間測定装置 5 2 で測定された時刻との時間差が所定範囲内であるか否かが判定されるが、認証情報として付加された時間情報は、情報認証装置 1 0 0 で生成された正当なものであるので、ここでは、その時間差が所定範囲内であると判定される。

【0 1 4 9】

次いで、ステップ S 2 0 6 を経て、復号化されたデジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置 5 4 で測定された位置を中心として所定範囲の領域内に含まれているか否かが判定されるが、認証情報として付加された位置情報は、情報認証装置 1 0 0 で生成された正当なものであるので、ここでは、位置情報により特定される位置が所定範囲の領域内に含まれると判定される。

【0 1 5 0】

次いで、ステップ S 2 0 8 ～ S 2 1 2 を経て、復号化されたデジタルデータの認証情報として付加された装置情報が復号化され、復号化された装置情報をもとに装置情報記憶装置 2 8 が検索され、復号化された装置情報に該当する装置情報が索出されたか否かが判定されるが、復号化された装置情報は、情報認証装置 1 0 0 で与えられた正当なものであることから、同一の装置情報が装置情報記憶装置 2 8 に登録されているので、ここでは、該当する装置情報が索出されたと判定される。

【0 1 5 1】

次いで、ステップ S 2 1 4 ～ S 2 1 8 を経て、復号化されたデジタルデータの認証情報として付加された個人情報が復号化され、索出された装置情報をもとに、個人情報記憶装置 2 6 が検索されて関連する個人情報が読み出され、復号化された個人情報である ID およびパスワードと、読み出された個人情報である ID およびパスワードと、が一致しているか否かが判定されるが、復号化された個

人情報は、情報認証装置 1 0 0 で与えられた正当なものであるので、ここでは、これらが一致していると判定される。

【0 1 5 2】

次いで、ステップ S 2 2 0, S 2 2 2 を経て、復号化されたデジタルデータのうち認証情報として付加された検査情報を除いた部分を用いて、ハッシュ関数により検査情報がハッシュ値として生成され、生成された検査情報と、復号化されたデジタルデータの認証情報として付加された検査情報と、が一致しているか否かが判定されるが、認証情報として付加された検査情報は、情報認証装置 1 0 0 で生成された正当なものであるので、ここでは、これらが一致していると判定される。

【0 1 5 3】

次いで、ステップ S 2 2 4 ~ S 2 2 8 を経て、復号化されたデジタルデータにデジタル署名が付加され、デジタル署名が付加されたデジタルデータが認証局 2 0 0 の秘密鍵で暗号化され、暗号化されたデジタルデータが通信装置 2 4 に出力される。そして、通信装置 2 4 により、ネットワークを介してデジタルデータが情報認証装置 1 0 0 に送信される。

【0 1 5 4】

一方、情報認証装置 1 0 0 では、通信装置 1 8 により、認証局 2 0 0 からデジタルデータが受信されると、受信されたデジタルデータが情報処理装置 4 0 に出力される。情報処理装置 4 0 では、デジタルデータが通信装置 1 8 から入力されると、CPU 6 0 により、ステップ S 1 2 6, S 1 2 8 を経て、入力されたデジタルデータがデータ記憶装置 2 0 に格納される。

【0 1 5 5】

ここで、利用者がデジタルデータの出力要求を行うと、ステップ S 1 3 0, S 1 3 2 を経て、データ記憶装置 2 0 のデジタルデータが出力端子 2 2 に出力される。出力端子 2 2 から出力されたデジタルデータは、例えば、フロッピーディスク等に記憶される。

【0 1 5 6】

なお、不正行為等により、認証情報が付加されたデジタルデータのうち、デ

デジタルデータ、時間情報、位置情報、個人情報、装置情報および検査情報のいずれかが改ざんされた場合は、認証局 2 0 0 において、ステップ S 2 0 4、S 2 0 6、S 2 1 2、S 2 1 8 および S 2 2 2 のいずれかのステップを経て、不正なデジタルデータであると判定され、デジタル署名が付加されない。

【0 1 5 7】

また、不正行為等により、認証局 2 0 0 で受信したデジタルデータが、そのデジタルデータの送信元である情報認証装置 1 0 0 の秘密鍵以外の鍵で暗号化されている場合には、認証局 2 0 0 において、ステップ S 2 0 2 を経て、デジタルデータが復号化されないため、不正なデジタルデータであるとして処理される。

【0 1 5 8】

また、不正行為等により、認証局 2 0 0 以外でデジタル署名が付加された場合には、情報認証装置 1 0 0 から出力されたデジタルデータが、認証局 2 0 0 の公開鍵で復号化することができないため、不正なデジタルデータであることが分かる。

【0 1 5 9】

また、情報認証装置 1 0 0 への電源投入時に、利用者が認証局 2 0 0 に届け出ていない不正な ID およびパスワードを入力した場合には、情報認証装置 1 0 0 において、ステップ S 1 0 2、S 1 3 4 を経て、強制的に電源が遮断される。

【0 1 6 0】

このようにして、本実施の形態では、情報認証装置 1 0 0 は、デジタルデータを取り込むデジタルカメラ 1 0 と、外部から取得した情報に基づいて認証情報を生成してこれをデジタルカメラ 1 0 で入力したデジタルデータに付加する認証情報付加部 1 2 0 と、を備えた。

【0 1 6 1】

これにより、内部で生成した情報に基づいて生成した認証情報を付加する場合に比して、デジタルデータに付加された認証情報が客観性を有するので、従来に比して、デジタルデータの客観性を確保することができ、デジタルデータの証拠としての証明力を向上することができる。

【 0 1 6 2 】

さらに、本実施の形態では、デジタルデータを取り込むデジタルカメラ 1 0 と、デジタルカメラ 1 0 で入力したデジタルデータに認証情報を付加する認証情報付加部 1 2 0 と、認証情報付加部 1 2 0 で認証情報を付加したデジタルデータを認証局 2 0 0 に送信する通信装置 1 8 と、を備えた。

【 0 1 6 3 】

これにより、内部で生成した情報に基づいて生成した認証情報を付加する場合に比して、デジタルデータに付加された認証情報が客観性を有するので、従来に比して、デジタルデータの客観性を確保することができ、デジタルデータの証拠としての証明力を向上することができる。

【 0 1 6 4 】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、時間測定装置 4 2 で測定した時間に基づいて時間情報を生成し、生成した時間情報を認証情報として付加するようにした。

【 0 1 6 5 】

これにより、デジタルデータに付加された認証情報から、デジタルデータを入力した時点を特定することができ、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【 0 1 6 6 】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、位置測定装置 4 4 で測定した位置に基づいて位置情報を生成し、生成した位置情報を認証情報として付加するようにした。

【 0 1 6 7 】

これにより、デジタルデータに付加された認証情報から、デジタルデータを入力した地点を特定することができ、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【 0 1 6 8 】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、センサ $S_1 \sim S_n$ で測定した環境状態に基づいて環境状態情報を生成し、生成した環境状態情報を認証情

報として付加するようにした。

【0 1 6 9】

これにより、デジタルデータに付加された認証情報から、デジタルデータを入力した時点における環境状態を特定することができ、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【0 1 7 0】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、個人情報入力装置 1 2 で入力した個人情報と個人情報記憶装置 1 4 の個人情報とが一致しているときは、個人情報記憶装置 1 4 の個人情報を認証情報として付加するようにした。

【0 1 7 1】

これにより、デジタルデータに付加された認証情報から、デジタルデータを入力した利用者を特定することができ、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【0 1 7 2】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、装置情報記憶装置 1 6 の装置情報を認証情報として付加するようにした。

【0 1 7 3】

これにより、デジタルデータに付加された認証情報から、デジタルデータを入力した装置を特定することができ、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【0 1 7 4】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、デジタルカメラ 1 0 で入力したデジタルデータを用いて検査情報を生成し、生成した検査情報を認証情報として付加するようにした。

【0 1 7 5】

これにより、デジタルデータに付加された認証情報から、デジタルデータが改ざんされているか否かが分かり、しかもその認証情報が客観性を有するので、デジタルデータの証拠としての証明力をさらに向上することができる。

【0 1 7 6】

さらに、本実施の形態では、認証情報付加部 1 2 0 は、公開鍵暗号化方式により、認証情報を付加したデジタルデータを情報認証装置 1 0 0 の秘密鍵で暗号化するようにした。

【0 1 7 7】

これにより、認証局 2 0 0 では、受信したデジタルデータが、そのデジタルデータの送信元である情報認証装置 1 0 0 の公開鍵でしか復号化することができないので、復号化できたときは、情報認証装置 1 0 0 で入力したデジタルデータが確かにその情報認証装置 1 0 0 から送信されたものであるということが分かり、復号化できなかったときは、そうでないことが分かるので、デジタルデータの証拠としての証明力をさらに向上することができる。

【0 1 7 8】

一方、本実施の形態では、認証局 2 0 0 は、情報認証装置 1 0 0 からデジタルデータを受信する通信装置 2 4 と、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するデジタル署名付加部 2 2 0 と、を備え、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータに付加された認証情報に基づいて、デジタルカメラ 1 0 でデジタルデータを入力したことを認証したときは、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようにした。

【0 1 7 9】

これにより、デジタルデータに付加された認証情報が改ざんされたりデジタルデータが不正な方法で送信されたりした場合には、デジタルデータにデジタル署名が付加されないので、従来に比して、デジタルデータの客観性を確保することができ、デジタルデータの証拠としての証明力を向上することができる。

【0 1 8 0】

さらに、本実施の形態では、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータの認証情報として付加された時間情報により特定される時間と時間測定装置 5 2 で測定した時間との時間差が所定範囲内であるときは

、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようにした。

【0 1 8 1】

これにより、デジタルデータの認証情報として付加された時間情報が改ざんされた場合には、デジタルデータにデジタル署名が付加されないので、デジタルデータの客観性をさらに確保することができ、デジタルデータの証拠としての証明力をより一層向上することができる。

【0 1 8 2】

さらに、本実施の形態では、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータの認証情報として付加された位置情報により特定される位置が、位置測定装置 5 4 で測定した位置を中心として所定範囲の領域内に含まれているときは、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようにした。

【0 1 8 3】

これにより、デジタルデータの認証情報として付加された位置情報が改ざんされた場合には、デジタルデータにデジタル署名が付加されないので、デジタルデータの客観性をさらに確保することができ、デジタルデータの証拠としての証明力をより一層向上することができる。

【0 1 8 4】

さらに、本実施の形態では、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータの認証情報として付加された装置情報と装置情報記憶装置 2 8 の装置情報とが一致しているときは、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようにした。

【0 1 8 5】

これにより、デジタルデータの認証情報として付加された装置情報が改ざんされた場合には、デジタルデータにデジタル署名が付加されないので、デジタルデータの客観性をさらに確保することができ、デジタルデータの証拠としての証明力をより一層向上することができる。

【 0 1 8 6 】

さらに、本実施の形態では、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータを用いて検査情報を生成し、生成した検査情報と通信装置 2 4 で受信したデジタルデータの認証情報として付加された検査情報とが一致しているときは、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようにした。

【 0 1 8 7 】

これにより、デジタルデータの認証情報として付加された検査情報やデジタルデータ自体が改ざんされた場合には、デジタルデータにデジタル署名が付加されないので、デジタルデータの客観性をさらに確保することができ、デジタルデータの証拠としての証明力をより一層向上することができる。

【 0 1 8 8 】

なお、上記実施の形態において、認証局 2 0 0 は、デジタル署名を付加したデジタルデータを情報認証装置 1 0 0 に送信する際に、デジタルデータに情報を付加するようには特に構成しなかったが、これに限らず、ステップ S 2 2 2 を経た後、通信装置 2 4 で受信したデジタルデータ（認証情報を含む。）を所定のハッシュ関数に代入することにより、そのデジタルデータに誤りが含まれているか否かを検査するための検査情報を、そのハッシュ関数により得られるハッシュ値として生成し、生成した検査情報をそのデジタルデータに付加するように構成してもよい。

【 0 1 8 9 】

このような構成であれば、情報認証装置 1 0 0 において、付加された検査情報によりデジタルデータの正当性を検証することができるので、デジタルデータの客観性をさらに確保することができ、デジタルデータの証拠としての証明力をより一層向上することができる。

【 0 1 9 0 】

また、上記実施の形態において、認証局 2 0 0 は、デジタル署名を付加したデジタルデータを情報認証装置 1 0 0 に送信し、情報認証装置 1 0 0 は、受信したデジタルデータをデータ記憶装置 2 0 に格納するように構成したが、これ

に限らず、認証局 2 0 0 は、デジタルデータを記憶するデータ記憶装置を備え、デジタル署名を付加したデジタルデータをデータ記憶装置に格納するように構成してもよい。この場合、情報認証装置 1 0 0 は、データ記憶装置 2 0 および出力端子 2 2 を設けずに構成することができる。

【0 1 9 1】

また、上記実施の形態において、情報認証装置 1 0 0 は、時間測定装置 4 2 を設け、認証情報として時間情報をデジタルデータに付加するように構成したが、これに限らず、時間測定装置 4 2 を設けず、時間情報を付加しないように構成することもできる。この場合、認証局 2 0 0 は、時間測定装置 5 2 を設けず、時間情報による判定を行わないように構成することができる。

【0 1 9 2】

また、上記実施の形態において、情報認証装置 1 0 0 は、位置測定装置 4 4 を設け、認証情報として位置情報をデジタルデータに付加するように構成したが、これに限らず、位置測定装置 4 4 を設けず、位置情報を付加しないように構成することもできる。この場合、認証局 2 0 0 は、位置測定装置 5 4 を設けず、位置情報による判定を行わないように構成することができる。

【0 1 9 3】

また、上記実施の形態において、情報認証装置 1 0 0 は、センサ $S_1 \sim S_n$ を設け、認証情報として環境状態情報をデジタルデータに付加するように構成したが、これに限らず、センサ $S_1 \sim S_n$ を設けず、環境状態情報を付加しないように構成することもできる。

【0 1 9 4】

また、上記実施の形態において、情報認証装置 1 0 0 は、個人情報入力装置 1 2、個人情報記憶装置 1 4 および利用者認証装置 4 6 を設け、認証情報として個人情報をデジタルデータに付加するように構成したが、これに限らず、これらの装置を設けず、個人情報を付加しないように構成することもできる。この場合、認証局 2 0 0 は、個人情報記憶装置 2 6 を設けず、個人情報による判定を行わないように構成することができる。

【 0 1 9 5 】

また、上記実施の形態において、情報認証装置 1 0 0 は、装置情報記憶装置 1 6 を設け、認証情報として装置情報をデジタルデータに付加するように構成したが、これに限らず、装置情報記憶装置 1 6 を設けず、装置情報を付加しないように構成することもできる。この場合、認証局 2 0 0 は、装置情報記憶装置 2 8 を設けず、装置情報による判定を行わないように構成することができる。

【 0 1 9 6 】

また、上記実施の形態において、情報認証装置 1 0 0 は、認証情報として検査情報をデジタルデータに付加するように構成したが、これに限らず、検査情報を付加しないように構成することもできる。この場合、認証局 2 0 0 は、検査情報による判定を行わないように構成することができる。

【 0 1 9 7 】

また、上記実施の形態において、情報認証装置 1 0 0 は、認証情報を付加したデジタルデータを暗号化して送信するように構成したが、これに限らず、認証情報を付加したデジタルデータを暗号化せずに送信するように構成することもできる。この場合、認証局 2 0 0 は、受信したデジタルデータを復号化しないように構成することができる。

【 0 1 9 8 】

また、上記実施の形態において、図 3 および図 5 のフローチャートに示す処理を実行するにあたってはいずれも、ROM 6 2, 7 2 にあらかじめ格納されている制御プログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムを RAM 6 4, 7 4 に読み込んで実行するようにしてもよい。

【 0 1 9 9 】

ここで、記憶媒体とは、RAM、ROM等の半導体記憶媒体、FD、HD等の磁気記憶型記憶媒体、CD、CDV、LD、DVD等の光学的読取方式記憶媒体、MO等の磁気記憶型／光学的読取方式記憶媒体であって、電子的、磁氣的、光学的等の読み取り方法のいかににかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【0 2 0 0】

上記実施の形態において、デジタルカメラ 1 0 は、請求項 1 ないし 6、9 または 1 0 記載のデータ入力手段に対応し、認証情報付加部 1 2 0 は、請求項 1 ないし 1 2 記載の認証情報付加手段に対応し、通信装置 1 8 は、請求項 3 記載の送信手段および請求項 1 3 記載の受信手段に対応し、時間測定装置 4 2 は、請求項 4 記載の時間測定手段に対応し、位置測定装置 4 4 は、請求項 2 または 5 記載の位置測定手段に対応している。

【0 2 0 1】

また、上記実施の形態において、センサ $S_1 \sim S_n$ は、請求項 6 記載の環境状態測定手段に対応し、個人情報入力装置 1 2 は、請求項 7 記載の個人情報入力手段に対応し、個人情報記憶装置 1 4 は、請求項 7 記載の個人情報記憶手段に対応し、装置情報記憶装置 1 6 は、請求項 8 記載の装置情報記憶手段に対応し、データ記憶装置 2 0 は、請求項 1 3 記載のデータ記憶手段に対応している。

【0 2 0 2】

また、上記実施の形態において、通信装置 2 4 は、請求項 1 4 ないし 2 1 記載の受信手段および請求項 2 3 記載の送信手段に対応し、デジタル署名付加部 2 2 0 は、請求項 1 4 ないし 2 3 記載のデジタル署名付加手段に対応し、時間測定装置 5 2 は、請求項 1 5 記載の認証局側時間測定手段に対応し、位置測定装置 5 4 は、請求項 1 6 記載の認証局側位置測定手段に対応し、装置情報記憶装置 2 6 は、請求項 1 7 記載の認証局側装置情報記憶手段に対応している。

【0 2 0 3】**【発明の効果】**

以上説明したように、本発明に係る請求項 1 ないし 1 3 記載の情報認証装置によれば、データに付加された認証情報が客観性を有するので、従来に比して、データの客観性を確保することができ、データの証拠としての証明力を向上することができるという効果が得られる。

【0 2 0 4】

さらに、本発明に係る請求項 4 記載の情報認証装置によれば、データに付加された認証情報から、データを入力した時点を特定することができ、しかもその認

証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 0 5】

さらに、本発明に係る請求項 2 または 5 記載の情報認証装置によれば、データに付加された認証情報から、データを入力した地点を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 0 6】

さらに、本発明に係る請求項 6 記載の情報認証装置によれば、データに付加された認証情報から、データを入力した時点における環境状態を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 0 7】

さらに、本発明に係る請求項 7 記載の情報認証装置によれば、データに付加された認証情報から、データを入力した利用者を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 0 8】

さらに、本発明に係る請求項 8 記載の情報認証装置によれば、データに付加された認証情報から、データを入力した装置を特定することができ、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 0 9】

さらに、本発明に係る請求項 9 または 1 0 記載の情報認証装置によれば、データに付加された認証情報から、データが改ざんされているか否かが分かり、しかもその認証情報が客観性を有するので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【0 2 1 0】

さらに、本発明に係る請求項 1 1 または 1 2 記載の情報認証装置によれば、認

証局では、受信したデータが、そのデータの送信元である情報認証装置の公開鍵でしか復号化することができないので、復号化できたときは、情報認証装置で入力したデータが確かにその情報認証装置から送信されたものであるということが分かり、復号化できなかったときは、そうでないことが分かるので、データの証拠としての証明力をさらに向上することができるという効果も得られる。

【 0 2 1 1 】

一方、本発明に係る請求項 1 4 ないし 2 3 記載の認証局によれば、データに付加された認証情報が改ざんされたりデータが不正な方法で送信されたりした場合には、データにデジタル署名が付加されないで、従来に比して、データの客観性を確保することができ、データの証拠としての証明力を向上することができるという効果が得られる。

【 0 2 1 2 】

さらに、本発明に係る請求項 1 5 記載の認証局によれば、データの認証情報として付加された時間情報が改ざんされた場合には、データにデジタル署名が付加されないで、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【 0 2 1 3 】

さらに、本発明に係る請求項 1 6 記載の認証局によれば、データの認証情報として付加された位置情報が改ざんされた場合には、データにデジタル署名が付加されないで、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【 0 2 1 4 】

さらに、本発明に係る請求項 1 7 記載の認証局によれば、データの認証情報として付加された装置情報が改ざんされた場合には、データにデジタル署名が付加されないで、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【 0 2 1 5 】

さらに、本発明に係る請求項 1 8 または 1 9 記載の認証局によれば、データの認証情報として付加された検査情報やデータ自体が改ざんされた場合には、デー

タにデジタル署名が付加されないので、データの客観性をさらに確保することができ、データの証拠としての証明力をより一層向上することができるという効果も得られる。

【図面の簡単な説明】

【図 1】

情報認証システムの構成を示すブロック図である。

【図 2】

情報処理装置 4 0 の構成を示すブロック図である。

【図 3】

認証情報付加処理を示すフローチャートである。

【図 4】

情報処理装置 5 0 の構成を示すブロック図である。

【図 5】

デジタル署名付加処理を示すフローチャートである。

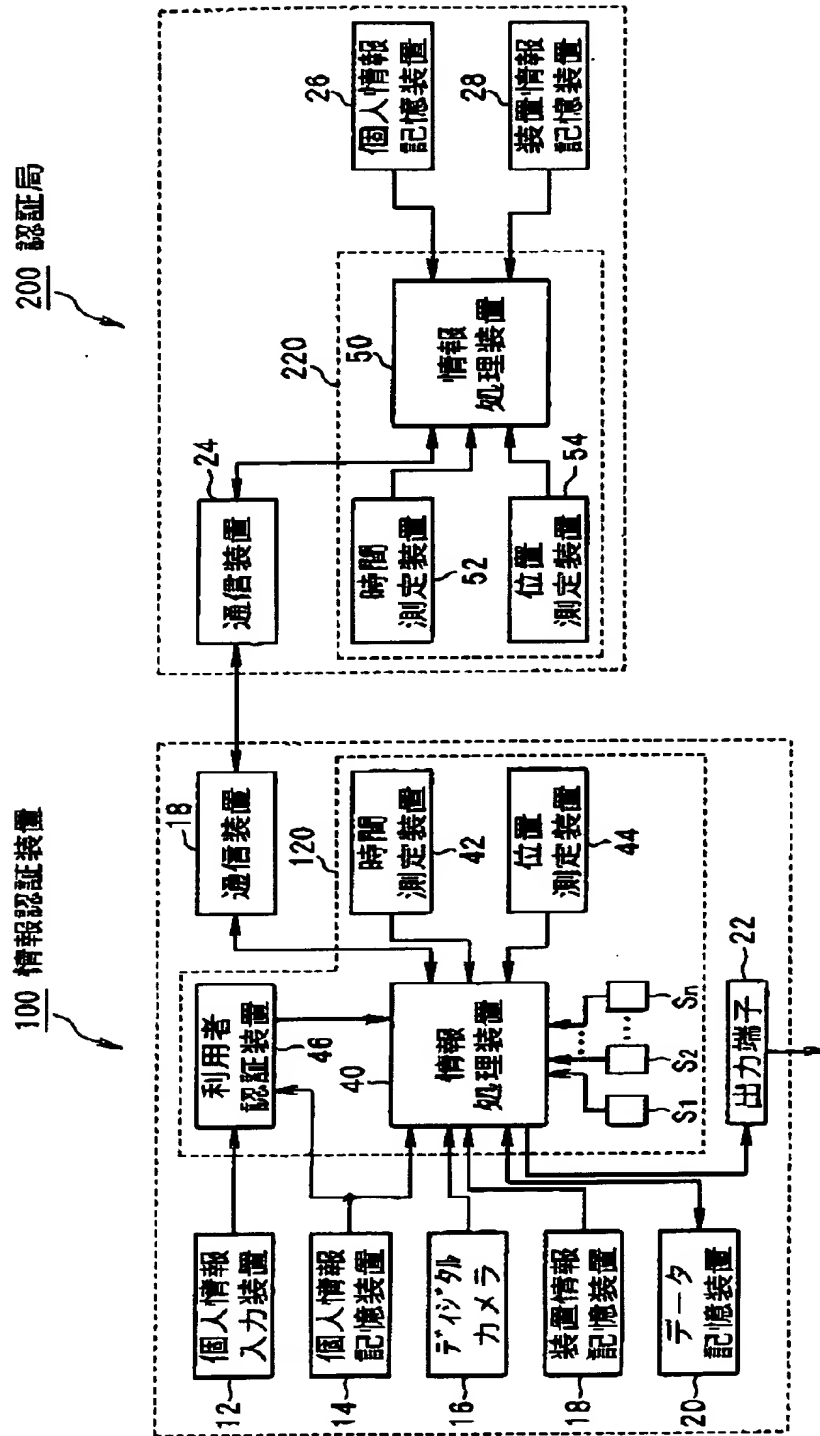
【符号の説明】

1 0 0	情報認証装置
1 2 0	認証情報付加部
2 0 0	認証局
2 2 0	デジタル署名付加部
1 0	デジタルカメラ
1 2, 2 6	個人情報入力装置
1 4	個人情報記憶装置
1 6, 2 8	装置情報記憶装置
1 8, 2 4	通信装置
2 0	データ記憶装置
4 0, 5 0	情報処理装置
4 2, 5 2	時間測定装置
4 4, 5 4	位置測定装置
S ₁ ～S _n	センサ

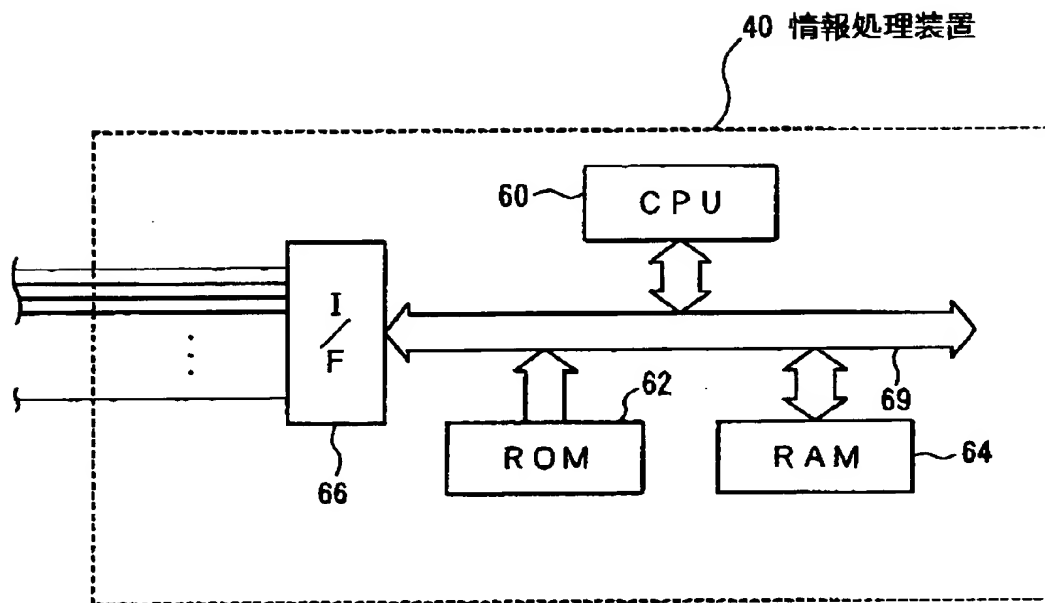
4 6	利用者認証装置
6 0 , 7 0	C P U
6 2 , 7 2	R O M
6 4 , 7 4	R A M

【書類名】 図面

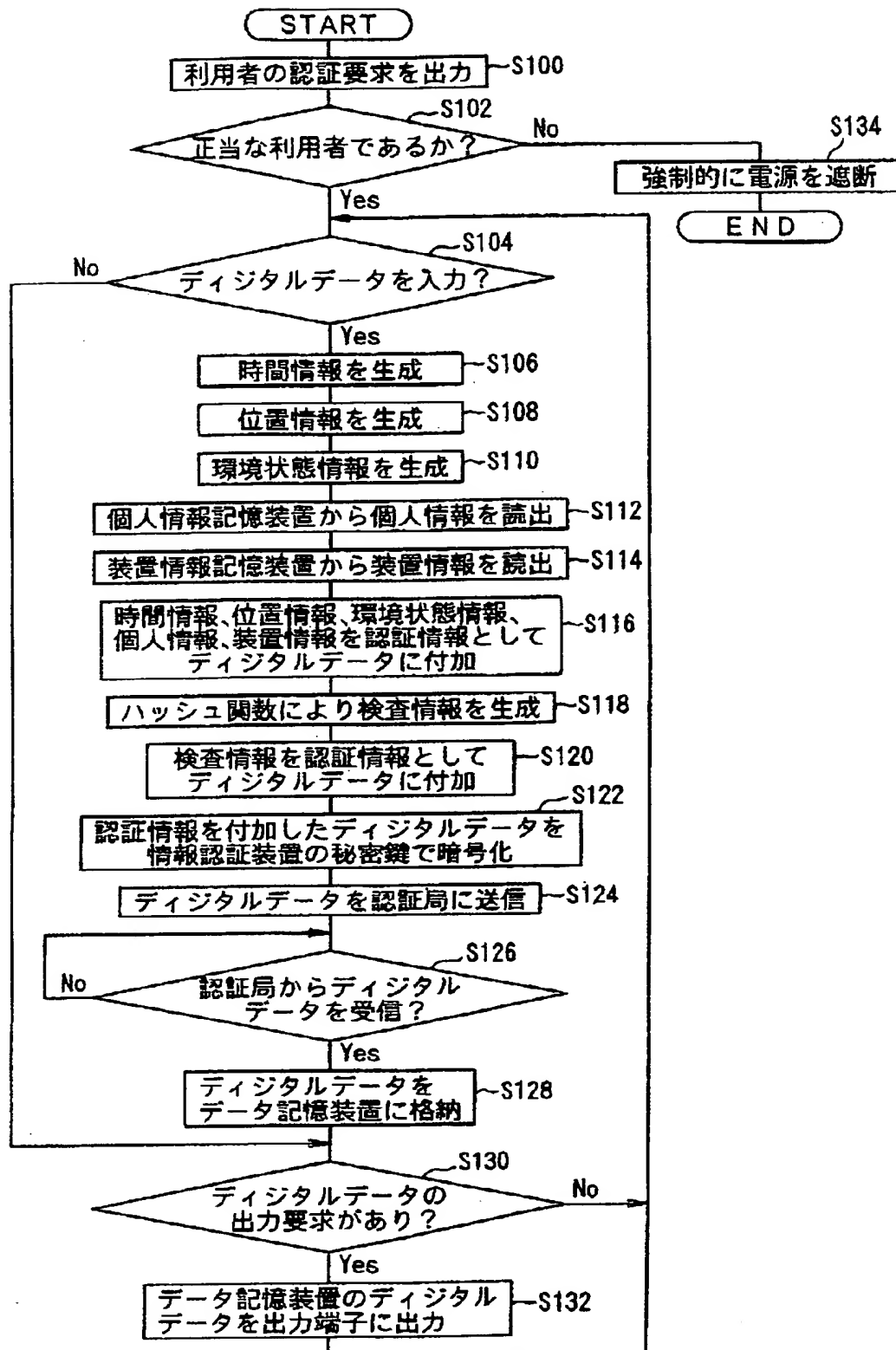
【図 1】



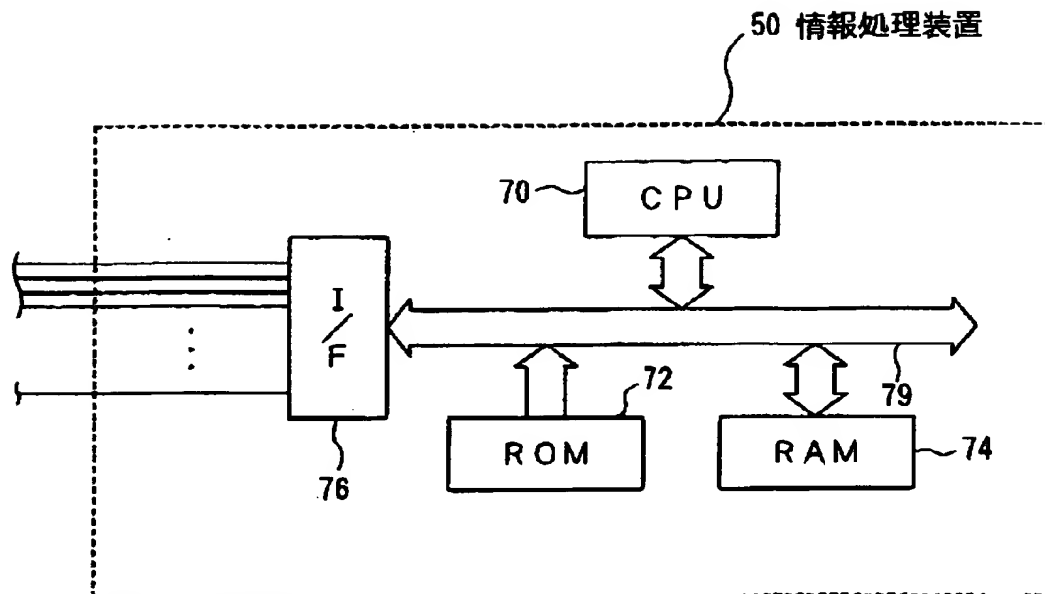
【図 2】



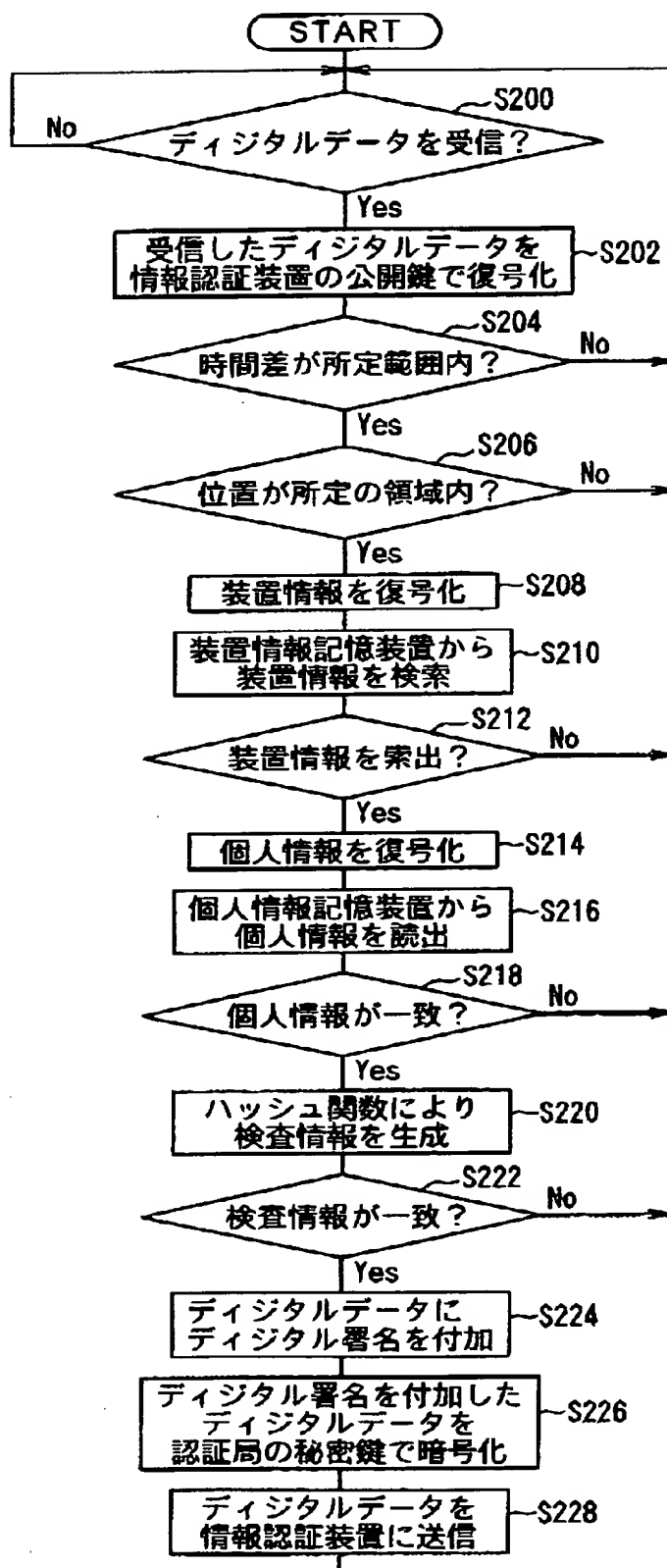
【図 3】



【図 4】



【図5】



【書類名】 要約書

【要約】

【課題】 データの客観性を確保することにより、データの証拠としての証明力を向上するのに好適な情報認証装置および認証局を提供する。

【解決装置】 情報認証装置 1 0 0 は、デジタルカメラ 1 0 と、デジタルカメラ 1 0 で入力したデジタルデータに認証情報を付加する認証情報付加部 1 2 0 と、で構成されている。一方、認証局 2 0 0 は、情報認証装置 1 0 0 からデジタルデータを受信する通信装置 2 4 と、デジタル署名付加部 2 2 0 と、を備え、デジタル署名付加部 2 2 0 は、通信装置 2 4 で受信したデジタルデータに付加された認証情報に基づいて、デジタルカメラ 1 0 でデジタルデータを入力したことを認証したときは、通信装置 2 4 で受信したデジタルデータにデジタル署名を付加するようになっている。

【選択図】 図 1

特願平 1 1 - 2 8 0 8 2 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 3 6 9]

1. 変更年月日

1 9 9 0 年 8 月 2 0 日

[変更理由]

新規登録

住 所

東京都新宿区西新宿 2 丁目 4 番 1 号

氏 名

セイコーエプソン株式会社